

## Act.03 - Interpretación y traducción de políticas de filtrado en iptables

## - CNO V. Seguridad Informática

Nombre: Miguel Angel Aguirre Cuurizales 182318  
 Fecha: 03 de Febrero de 2016 Calf: \_\_\_\_\_

- Completa los espacios conforme se explica el flujo del paquete.

Cuando un paquete llega al sistema, primero pasa por una table, después por una queue y finalmente se ejecuta una Rule/acción

- Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Que paquetes pasar o no	Permitir / Bloquear
NAT	Traducción de direcciones	Port Forwarding
MANGLE	Manipulación de paquetes	Comprimir cabeceras
RAW	Excepción de segmentación	Auditar paquetes
SECURITY	Aplicar etiquetas de seguridad Se anotara servicio	Contexto de seguridad

- Anatomía de un comando iptables:  
`iptables -A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT`

4. Este comando permite:

Crear una regla que acepte todo lo que llega de entrada que sea TCP a los puertos 80 y 443

5. Variables y opciones comunes

a) Limitar intentos por minuto

`--limit 5/min`

b) Filtrar por IP de origen

`-s 0 source`

c) Ver solo números, sin DNS (ni resolución de puertos)

`-n`

d) Ver reglas con contadores (paquetes y bytes)

`-l list -v`

6. ¿Qué hace esta regla?

`iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 \ -m state --state NEW,ESTABLISHED -j ACCEPT`

Crear una regla para la tabla filter y que acepte mientras llegue de la interfaz ethernet con protocolo TCP y conexión nuevo establecido, que este establecido mientras llegue a los puertos 22(SSH), 80(CHATP) y 443(HTTPS)

7. Permitir tráfico HTTP entrante  
-A INPUT -p tcp -m multiport --dports 80 -j ACCEPT
8. Permitir todo el tráfico saliente  
-A OUTPUT -p tcp -j ACCEPT
9. Permitir SSH solo desde la IP 192.168.1.50  
-A INPUT -p tcp -o -dport 22 -s 192.168.1.50 -j ACCEPT
10. Permitir tráfico TCP entrante a puertos 80 y 443 solo si es conexión establecida o relacionada  
-A INPUT -p tcp -m multiport --dports 80,443 -m state  
state ESTABLISHED -j ACCEPT
11. Permitir tráfico TCP entrante por eth0 a 22, 80 y 443, registrar intentos y permitir solo NEW  
y ESTABLISHED  
-A INPUT -p tcp -i eth0 -m multiport --dports 22,80,443  
state -m state NEW,ESTABLISHED -j LOG -l LOG -t log\_level=2 -f  
ACCEPT